JP2005109861

Publication Title:

ENCRYPTING DEVICE OF TRANSPORT STREAM, AND EDITING DEVICE, AND METHODS FOR THEM

Abstract:

Abstract of JP2005109861

PROBLEM TO BE SOLVED: To edit contents with the copyright of the contents protected.
SOLUTION: An encrypting device is provided with a detecting means for detecting a TS (transport stream) header of an unencrypted transport stream, PES (packetized elementary stream) header, sequence header, GOP (group of picture) header and sequence end code, and an encrypting means for encrypting a transport stream excluding the TS header, PES header, sequence header, GOP header, and sequence end code. An editing device is provided with: a detecting means for detecting the TS header of a transport stream, PES header, sequence header, GOP header and sequence end code; and an editing means for editing an encrypted transport stream among TS packets having one and the same PID with a TS packet from which the GOP header is detected to a TS packet preceding a TS packet with the next GOP header detected as a unit without decrypting the encrypted transport stream.
COPYRIGHT: (C)2005,JPO&NCIPI

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-109861
(P2005-109861A)
(43)公開日　平成17年4月21日(2005.4.21)

(51) Int.Cl.[7]	F I		テーマコード（参考）
H04N 7/167	H04N 7/167	Z	5C053
H04L 9/36	H04N 5/91	N	5C064
H04N 5/91	H04N 5/92	H	5J104
H04N 5/92	H04L 9/00	685	

審査請求 有　請求項の数 19　OL　（全 14 頁）

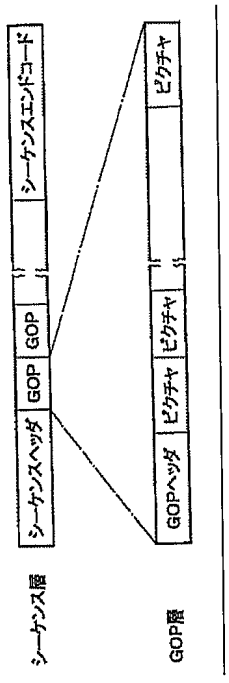
(21)出願番号　特願2003-340338 (P2003-340338)
(22)出願日　平成15年9月30日 (2003.9.30)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100065385
弁理士　山下　穣平
(74)代理人　100122921
弁理士　志村　博
(74)代理人　100130029
弁理士　永井　道雄
(74)代理人　100065385
弁理士　山下　穣平
(72)発明者　酒井　祐一
東京都港区芝五丁目７番１号　日本電気株式会社内

最終頁に続く

(54)【発明の名称】トランスポートストリームの暗号化装置及び編集装置並びにこれらの方法

(57)【要約】
【課題】　コンテンツの著作権を保護したまま、コンテンツの編集をする。
【解決手段】　暗号化装置は、非暗号化トランスポートストリームのＴＳヘッダ、ＰＥＳヘッダ、シーケンスヘッダ、ＧＯＰヘッダ及びシーケンスエンドコードを検出する検出手段と、ＴＳヘッダ、ＰＥＳヘッダ、シーケンスヘッダ、ＧＯＰヘッダ及びシーケンスエンドコードを除いてトランスポートストリームを暗号化する暗号化手段を備える。編集装置は、トランスポートストリームのＴＳヘッダ、ＰＥＳヘッダ、シーケンスヘッダ、ＧＯＰヘッダ及びシーケンスエンドコードを検出する検出手段と、同一のＰＩＤを有するＴＳパケットのうち、ＧＯＰヘッダが検出されたＴＳパケットから次のＧＯＰヘッダが検出されたＴＳパケットの前のＴＳパケットまでを単位として、暗号化されたトランスポートストリームを暗号解読せずに編集する編集手段を備える。
【選択図】　図４



【特許請求の範囲】
【請求項1】
入力ストリームから編集単位のヘッダ及び前記ヘッダを検出するために必要な部分を少なくとも検出する検出手段と、
前記ヘッダ及び前記ヘッダを検出するための部分を少なくとも除いて前記入力ストリームを暗号化する暗号化手段と、
を備えることを特徴とするストリームの暗号化装置。
【請求項2】
請求項１に記載のストリーム暗号化装置により暗号化されたストリームから前記ヘッダを検出するために必要な部分及び前記ヘッダを検出する検出手段と、
前記編集単位で前記ストリームを暗号化されたままの状態で編集する編集手段と、
を備えることを特徴とするストリームの編集装置。
【請求項3】
暗号化されていないトランスポートストリームのＴＳヘッダ、ＴＳパケットのペイロードに在るＰＥＳパケットのＰＥＳヘッダ及びビデオＰＥＳパケットのペイロードに在るＧＯＰヘッダを少なくとも検出する検出手段と、
検出された前記ＴＳヘッダ、前記ＰＥＳヘッダ及び前記ＧＯＰヘッダを少なくとも除いて前記トランスポートストリームを暗号化する暗号化手段と、
を備えることを特徴とするトランスポートストリームの暗号化装置。
【請求項4】
請求項３に記載のトランスポートストリームの暗号化装置において、
前記検出手段は、前記ビデオＰＥＳパケットのペイロードに在るシーケンスヘッダ及びシーケンスエンドコードも検出し、
前記暗号化手段は、検出された前記シーケンスヘッダ及び前記シーケンスエンドコードも除いて前記トランスポートストリームを暗号化することを特徴とするトランスポートストリームの暗号化装置。
【請求項5】
請求項３に記載の暗号化装置において、
前記暗号化手段は、異なったＧＯＰを含むＴＳパケットを異なった暗号鍵で暗号化することを特徴とするトランスポートストリームの暗号化装置。
【請求項6】
請求項３に記載の暗号化装置において、
前記暗号化されていないトランスポートストリーム又は前記暗号化されたトランスポートストリームから動画像を復元する動画像復元手段と、
前記復元された動画像を基に全部又は一部のＧＯＰのそれぞれに対応した代表画像を生成する代表画像生成手段と、
を更に備えることを特徴とするトランスポートストリームの暗号化装置。
【請求項7】
請求項３に記載のトランスポートストリームの暗号化装置により暗号化されたトランスポートストリームのＴＳヘッダ、ＴＳパケットのペイロードに在るＰＥＳパケットのＰＥＳヘッダ及びビデオＰＥＳパケットのペイロードに在るＧＯＰヘッダを検出する検出手段と、
同一のＰＩＤを有するＴＳパケットのうち、ＧＯＰヘッダが検出されたＴＳパケットから次のＧＯＰヘッダが検出されたＴＳパケットの前のＴＳパケットまでを単位として、前記暗号化されたトランスポートストリームを暗号解読せずに編集する編集手段と、
を備えることを特徴とするトランスポートストリームの編集装置。
【請求項8】
請求項３に記載のトランスポートストリームの暗号化装置により暗号化されたトランスポートストリームのＴＳヘッダ、ＴＳパケットのペイロードに在るＰＥＳパケットのＰＥ

Ｓヘッダ及びビデオＰＥＳパケットのペイロードに在るＧＯＰヘッダを検出する検出手段と、
同一のＰＩＤを有するＴＳパケットのうち、ＧＯＰヘッダが検出されたＴＳパケットから次のＧＯＰヘッダが検出されたＴＳパケットの前のＴＳパケットまでを単位として、前記代表画像を参照してユーザにより選択されたＧＯＰが含まれるように、前記暗号化されたトランスポートストリームを暗号解読せずに編集する編集手段と、
を備えることを特徴とするトランスポートストリームの編集装置。
【請求項9】
請求項７又は８に記載のトランスポートストリームの編集装置において、
前記検出手段は、前記ビデオＰＥＳパケットのペイロードにあるシーケンスヘッダ及びシーケンスエンドコードも検出することを特徴とするトランスポートストリームの編集装置。
【請求項10】
入力ストリームから編集単位のヘッダ及び前記ヘッダを検出するために必要な部分を少なくとも検出する検出ステップと、
前記ヘッダ及び前記ヘッダを検出するための部分を少なくとも除いて前記入力ストリームを暗号化する暗号化ステップと、
を備えることを特徴とするストリームの暗号化方法。
【請求項11】
請求項１０に記載のストリーム暗号化方法により暗号化されたストリームから前記ヘッダを検出するために必要な部分及び前記ヘッダを検出する検出ステップと、
前記編集単位で前記ストリームを暗号化されたままの状態で編集する編集ステップと、
を備えることを特徴とするストリームの編集方法。
【請求項12】
暗号化されていないトランスポートストリームのＴＳヘッダ、ＴＳパケットのペイロードに在るＰＥＳパケットのＰＥＳヘッダ及びビデオＰＥＳパケットのペイロードに在るＧＯＰヘッダを少なくとも検出する検出ステップと、
検出された前記ＴＳヘッダ、前記ＰＥＳヘッダ及び前記ＧＯＰヘッダを少なくとも除いて前記トランスポートストリームを暗号化する暗号化ステップと、
を備えることを特徴とするトランスポートストリームの暗号化方法。
【請求項13】
請求項１２に記載のトランスポートストリームの暗号化方法において、
前記検出ステップは、前記ビデオＰＥＳパケットのペイロードに在るシーケンスヘッダ及びシーケンスエンドコードも検出し、
前記暗号化ステップは、検出された前記シーケンスヘッダ及び前記シーケンスエンドコードも除いて前記トランスポートストリームを暗号化することを特徴とするトランスポートストリームの暗号化方法。
【請求項14】
請求項１２に記載の暗号化方法において、
前記暗号化ステップは、異なったＧＯＰを含むＴＳパケットを異なった暗号鍵で暗号化することを特徴とするトランスポートストリームの暗号化方法。
【請求項15】
請求項１２に記載の暗号化方法において、
前記暗号化されていないトランスポートストリーム又は前記暗号化されたトランスポートストリームから動画像を復元する動画像復元ステップと、
前記復元された動画像を基に全部又は一部のＧＯＰのそれぞれに対応した代表画像を生成する代表画像生成ステップと、
を更に備えることを特徴とするトランスポートストリームの暗号化方法。
【請求項16】
請求項１２に記載のトランスポートストリームの暗号化方法により暗号化されたトラン

スポートストリームのＴＳヘッダ、ＴＳパケットのペイロードに在るＰＥＳパケットのＰＥＳヘッダ及びビデオＰＥＳパケットのペイロードに在るＧＯＰヘッダを検出する検出ステップと、

同一のＰＩＤを有するＴＳパケットのうち、ＧＯＰヘッダが検出されたＴＳパケットから次のＧＯＰヘッダが検出されたＴＳパケットの前のＴＳパケットまでを単位として、前記暗号化されたトランスポートストリームを暗号解読せずに編集する編集ステップと、

を備えることを特徴とするトランスポートストリームの編集方法。

【請求項17】

請求項１２に記載のトランスポートストリームの暗号化方法により暗号化されたトランスポートストリームのＴＳヘッダ、ＴＳパケットのペイロードに在るＰＥＳパケットのＰＥＳヘッダ及びビデオＰＥＳパケットのペイロードに在るＧＯＰヘッダを検出する検出ステップと、

同一のＰＩＤを有するＴＳパケットのうち、ＧＯＰヘッダが検出されたＴＳパケットから次のＧＯＰヘッダが検出されたＴＳパケットの前のＴＳパケットまでを単位として、前記代表画像を参照してユーザにより選択されたＧＯＰが含まれるように、前記暗号化されたトランスポートストリームを暗号解読せずに編集する編集ステップと、

を備えることを特徴とするトランスポートストリームの編集方法。

【請求項18】

請求項１６又は１７に記載のトランスポートストリームの編集方法において、

前記検出ステップは、前記ビデオＰＥＳパケットのペイロードにあるシーケンスヘッダ及びシーケンスエンドコードも検出することを特徴とするトランスポートストリームの編集方法。

【請求項19】

コンピュータに請求項１０乃至１８のいずれか１項に記載の方法を行わせるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ＭＰＥＧ(Moving Picture Experts Group)信号を含むトランスポートストリームの暗号化装置及び編集装置並びにこれらの方法に関する。

【背景技術】

【0002】

近年、デジタル信号処理技術の進歩に伴い、映像信号は、デジタル信号の形態で伝送及び蓄積がされるようになってきている。デジタル信号の伝送及び蓄積の方式としては、ＭＰＥＧ方式が標準化されている。

【0003】

図１に、パーソナルコンピュータをベースとしたＭＰＥＧ信号の処理システムの従来例を示す。

【0004】

図１を参照すると、このシステムは、ＣＰＵ９０１、ハードディスクドライブ９０２、デジタル放送処理ボード９０３、汎用バス９０４及び表示部９０５を備える。

【0005】

ＣＰＵ９０１は、プログラムに従って、各種演算処理を行う。ハードディスクドライブ９０２は、各種プログラムやデータを格納し、特に、暗号化されたトランスポートストリームを格納する。デジタル放送処理ボード９０３は、デジタル放送より受信したトランスポートストリームの各種処理を行う。汎用バス９０４は、ＣＰＵ９０１、ハードディスクドライブ９０２及びデジタル放送処理ボード９０３に接続され、これらの間で入出力するデータを運ぶ。表示部９０５は、各種画面を表示し、特にデジタル放送処理ボード９０３から出力された映像信号を入力し、その映像信号に従って映像を表示する。

【0006】

デジタル放送処理ボード９０３は、受信部９１１、暗号化部９１２、暗号解読部９１３

及びＭＰＥＧデコーダ９１４を備える。

【0007】

受信部９１１は、放送よりトランスポートストリームを受信する。暗号化部９１２は、受信部９１１が受信したトランスポートストリームを暗号化して、暗号化されたトランスポートストリームを汎用バス９０４に出力する。ハードディスクドライブ９０２はこの暗号化されたトランスポートストリームを格納する。ハードディスクドライブ９０２は、格納されている暗号化されたトランスポートストリームを出力する。暗号解読部９１３は、この暗号化されたトランスポートストリームの暗号解読を行い、暗号解読されたトランスポートストリームから映像部分を多重分離したＭＰＥＧビットストリームをＭＰＥＧデコーダ９１４に出力する。

【0008】

ＭＰＥＧデコーダ９１４は、ＭＰＥＧビットストリームを復号して、これにより得た映像信号を表示部９０５に出力する。

【0009】

このような構成によれば、汎用バス９０４に現れるトランスポートストリームは暗号化されているので、汎用バス９０４に現れたトランスポートストリームを不正にコピーすることができない。また、ＭＰＥＧデコーダ９１４から出力された映像信号は直接表示部９０５に出力されるので、傍受することができない。このようにしてコンテンツの著作権を保護することができる。

【0010】

なお、本発明に関連する先行技術文献として、以下のものがある。

【特許文献1】特開平０８－３２２０３４号公報

【特許文献2】特開平１０－３３６６２４号公報

【特許文献3】特開２００２－２８７６２４号公報

【特許文献4】特開２００２－２８７６２５号公報

【特許文献5】特開２００２－２９０９９９号公報

【発明の開示】

【発明が解決しようとする課題】

【0011】

しかしながら、図１に示すようなシステムを用いた場合、トランスポートストリームが暗号化部９１２により完全に暗号化されてしまうので、暗号解読部９１３により暗号解読を行わない限り、トランスポートストリームのどの部分にどのような映像が入っているのかを知ることができない。従って、暗号解読部９１３により暗号解読を行わない限り、コンテンツの編集をすることができない。

【0012】

つまり、暗号解読部９１３によって暗号解読したトランスポートストリームを図１で破線で示す編集部９０６により編集することとすると、ハードディスクドライブ９０２から読み出されたデータは、暗号解読部９１３で暗号解読された後、編集部９０６で処理された後に、暗号化部９１２で暗号化され、ハードディスクドライブ９０２に再書き込みされるため、暗号解読されたトランスポートストリームが図１で破線矢印で示すように汎用バス９０４に現れることとなり、著作権を保護することができなくなってしまう。

【0013】

また、暗号化部９１２が暗号化する前のトランスポートストリームから各ＧＯＰの代表画像を得て、その代表画像を見ながら編集することも考えられるが、このＧＯＰを編集後のトランスポートストリームに含めたいことを希望しても、そのＧＯＰがトランスポートストリームのどこにあるのかが不明であり、それを明らかにするためには、結局は、暗号化されているトランスポートストリームを暗号解読しなければならず、著作権の保護を図ることができない。

【0014】

そこで、本発明は、コンテンツの著作権を保護したまま、コンテンツの編集をすること

を可能とするトランスポートストリームの暗号化装置及び編集装置並びにそれらの方法を提供することを目的とする。

【課題を解決するための手段】

【0015】

本発明の第１の観点によれば、入力ストリームから編集単位のヘッダ及び前記ヘッダを検出するために必要な部分を少なくとも検出する検出手段と、前記ヘッダ及び前記ヘッダを検出するための部分を少なくとも除いて前記入力ストリームを暗号化する暗号化手段と、を備えることを特徴とするストリームの暗号化装置が提供される。

【0016】

本発明の第２の観点によれば、本発明の第１の観点によるストリーム暗号化装置により暗号化されたストリームから前記ヘッダを検出するために必要な部分及び前記ヘッダを検出する検出手段と、前記編集単位で前記ストリームを暗号化されたままの状態で編集する編集手段と、を備えることを特徴とするストリームの編集装置が提供される。

【0017】

本発明の第３の観点によれば、暗号化されていないトランスポートストリームのＴＳヘッダ、ＴＳパケットのペイロードに在るＰＥＳパケットのＰＥＳヘッダ及びビデオＰＥＳパケットのペイロードに在るＧＯＰヘッダを少なくとも検出する検出手段と、検出された前記ＴＳヘッダ、前記ＰＥＳヘッダ及び前記ＧＯＰヘッダを少なくとも除いて前記トランスポートストリームを暗号化する暗号化手段と、を備えることを特徴とするトランスポートストリームの暗号化装置が提供される。

【0018】

本発明の第３の観点によるトランスポートストリームの暗号化装置において、前記検出手段は、前記ビデオＰＥＳパケットのペイロードに在るシーケンスヘッダ及びシーケンスエンドコードも検出し、前記暗号化手段は、検出された前記シーケンスヘッダ及び前記シーケンスエンドコードも除いて前記トランスポートストリームを暗号化してもよい。上記の暗号化装置において、前記暗号化手段は、異なったＧＯＰを含むＴＳパケットを異なった暗号鍵で暗号化してもよい。

【0019】

上記の暗号化装置は、前記暗号化されていないトランスポートストリーム又は前記暗号化されたトランスポートストリームから動画像を復元する動画像復元手段と、前記復元された動画像を基に全部又は一部のＧＯＰのそれぞれに対応した代表画像を生成する代表画像生成手段と、を更に備えていてもよい。

【0020】

本発明の第４の観点によれば、本発明の第１の観点によるトランスポートストリームの暗号化装置により暗号化されたトランスポートストリームのＴＳヘッダ、ＴＳパケットのペイロードに在るＰＥＳパケットのＰＥＳヘッダ及びビデオＰＥＳパケットのペイロードに在るＧＯＰヘッダを検出する検出手段と、同一のＰＩＤを有するＴＳパケットのうち、ＧＯＰヘッダが検出されたＴＳパケットから次のＧＯＰヘッダが検出されたＴＳパケットの前のＴＳパケットまでを単位として、前記暗号化されたトランスポートストリームを暗号解読せずに編集する編集手段と、を備えることを特徴とするトランスポートストリームの編集装置が提供される。

【0021】

本発明の第５の観点によれば、本発明の第１の観点によるトランスポートストリームの暗号化装置により暗号化されたトランスポートストリームのＴＳヘッダ、ＴＳパケットのペイロードに在るＰＥＳパケットのＰＥＳヘッダ及びビデオＰＥＳパケットのペイロードに在るＧＯＰヘッダを検出する検出手段と、同一のＰＩＤを有するＴＳパケットのうち、ＧＯＰヘッダが検出されたＴＳパケットから次のＧＯＰヘッダが検出されたＴＳパケットの前のＴＳパケットまでを単位として、前記代表画像を参照してユーザにより選択されたＧＯＰが含まれるように、前記暗号化されたトランスポートストリームを暗号解読せずに編集する編集手段と、を備えることを特徴とするトランスポートストリームの編集装置が

提供される。

【0022】

本発明の第４の観点又は第５の観点によるトランスポートストリームの編集装置において、前記検出手段は、前記ビデオＰＥＳパケットのペイロードにあるシーケンスヘッダ及びシーケンスエンドコードも検出してもよい。

【発明の効果】

【0023】

請求項１及び２に記載の発明によれば、暗号化されたストリームを暗号解読されなくてもストリームを編集単位で編集することが可能となるので、コンテンツの著作権を保護することが可能となる。

【0024】

請求項３に記載の発明によれば、ＴＳヘッダ、ＰＥＳヘッダ並びにシーケンスヘッダ、ＧＯＰヘッダ及びシーケンスエンドコードを除いてトランスポートストリームが暗号化されるので、暗号解読されなくても、ＴＳヘッダ、ＰＥＳヘッダ及ＧＯＰヘッダを検出することが可能となり、従って、コンテンツの著作権を保護した状態で、コンテンツの編集をすることが可能となる。

【0025】

請求項４に記載の発明によれば、異なったＧＯＰを含むＴＳパケットを異なった暗号鍵で暗号化するので、コンテンツの著作権をより厚く保護することができる。

【0026】

請求項５に記載の発明によれば、動画像を復元し、復元された動画像を基に全部又は一部のＧＯＰのそれぞれに対応した代表画像を生成するので、編集時のユーザインターフェースを容易にすることができる。

【0027】

請求項６に記載の発明によれば、暗号解読せずに編集を行うので、コンテンツの著作権を保護した状態で、コンテンツの編集をすることができる。

【0028】

請求項７に記載の発明によれば、暗号解読せずに編集を行うので、コンテンツの著作権を保護した状態で、コンテンツの編集をすることができると共に、代表画像を参照してユーザにより選択されたＧＯＰが含まれるように編集を行うので、ユーザインターフェースを容易にすることができる。

【発明を実施するための最良の形態】

【0029】

以下、図面を参照して本発明を実施するための最良の形態について説明する。

【0030】

図２は、トランスポートストリームのフォーマット図を示す。図２を参照すると、トランスポートストリームは、複数のＴＳ(Transport Stream)パケットより構成される。各ＴＳパケットは、固定長であり、ＴＳヘッダとＴＳペイロードより構成される。後述するＰＥＳ(Packetized Elementary Stream)は、一般に可変長であり、ＴＳパケットより長い。従って、１つのＰＥＳパケットは分割され、複数のＴＳパケットのペイロードに跨って挿入される。新たなＰＥＳパケットが始まるときには、新たなＴＳパケットが用いられ、従って、ＰＥＳヘッダは、必ずＴＳペイロードの先頭に在る。また、分割されたＰＥＳパケットのうち最後の分割されたＰＥＳパケットの長さがＴＳパケットのペイロードの長さよりも短い場合には、ＰＥＳパケットの前にスタッフィングバイトが挿入され、ＴＳパケットの長さが維持される。各ＰＥＳパケットは、ＰＥＳヘッダとＰＥＳペイロードより構成される。ＰＥＳペイロードには、分断化されたエレメンタリーストリームが挿入される。特に、ビデオエレメンタリーストリームから作成されたＰＥＳパケットのことをビデオＰＥＳパケットという。

【0031】

図３は、ＧＯＰ(Group Of Picture)及びビデオＰＥＳパケットのペイロードを示す。Ｇ

ＯＰの先頭には、ＧＯＰヘッダが配置される。ビデオエレメンタリーストリームをどのように分断化してビデオＰＥＳパケットを作成するのかは自由であるが、ＰＥＳパケットの先頭がＧＯＰの先頭と一致すると復号処理が容易となる。本実施形態では、図３に示すように、ＰＥＳパケットの先頭がＧＯＰの先頭と一致することとする。１つのＰＥＳパケットに含まれるピクチャ数は任意であるが、例えば、１つのＰＥＳパケットに１つのピクチャが含まれる。

【0032】

ＴＳヘッダには、ＰＩＤ等が含まれる。同一のＰＥＳパケットから生成されたＴＳパケットのＰＩＤは同一である。ＰＥＳヘッダには、ストリームＩＤ、ＰＥＳパケットレングス、ＰＴＳ(presentation time stamp)、ＤＴＳ(decoding time stamp)等が含まれる。１つのエレメンタリストリームは同一のストリームＩＤを持つＰＥＳパケットにより伝送される。そして、映像信号に対しては、０ｘＥ０～０ｘＦＥの範囲の値のストリームＩＤが割り当てられる。従って、ＴＳヘッダに含まれるＰＩＤ及びＰＥＳヘッダに含まれるストリームＩＤを調べることにより、どのＴＳパケットにどの系統の映像信号が含まれているのかを知ることができる。従って、ＴＳヘッダに含まれるＰＩＤ及びＰＥＳヘッダに含まれるストリームＩＤを調べることにより、着目している系統の映像信号のみを抜き出すことができる。

【0033】

ＧＯＰヘッダには、グループスタートコード、タイムコード（時、分、秒、ピクチャ）、クローズドＧＯＰ、ブロークンリンクが含まれる。

【0034】

編集は、ＧＯＰヘッダに含まれるタイムコードを基準として行われる。従って、編集を行うためには、ＧＯＰに含まれるタイムコードを検出しなければならない。トランスポートストリームからＧＯＰヘッダを検出するためには、まず、トランスポートストリームからＴＳヘッダを検出することにより各ＴＳパケットを認識し、認識されたＴＳパケットのペイロードのうちの一部のものの先頭に挿入されているＰＥＳヘッダを検出することによりＰＥＳパケットを認識し、認識されたＰＥＳパケットのうちビデオＰＥＳをつなぎ合わせてビデオエレメンタリストリームを再構築し、再構築されたビデオエレメンタリストリームからＧＯＰを再構成しなければならない。このような方法によりＧＯＰヘッダを検出した場合には、どのＴＳパケットにＧＯＰヘッダが含まれているのかを知ることができる。また上述したように、着目している系統の映像信号のみを抜き出すことができる。従って、着目している系統の映像信号のあるタイムコードからあるタイムコードまでの部分を含むＴＳパケットを抽出することができる。そして、抽出したＴＳパケットをつなぎ合わせ、その後、ＴＳヘッダとＰＥＳパケットの間にオプションで挿入されているアダプテーションフィールドに含まれるＰＣＲ(Program Clock Reference)並びにＰＥＳヘッダに含まれているＰＴＳ及びＤＴＳを調整することにより、編集を行うことができる。

【0035】

また、図４に示すように、１以上のＧＯＰ並びにシーケンスヘッダ及びシーケンスエンドコードはシーケンス層を構成する。シーケンスヘッダには、シーケンスヘッダコード、画面の縦横のサイズ、画面のアスペクト比、画像レート、ビットレート、ＶＢＶバッファサイズ及び量子化マトリックスが含まれる。そして、このようなシーケンスヘッダに含まれる情報は、編集後のＴＳストリームでそのまま引き継がなくてはならない。従って、ＧＯＰ単位で編集をする場合であっても、シーケンス層を認識する必要がある。

【0036】

従って、本実施形態では、コンテンツが暗号化されたままの状態で、編集をすることを可能とするために、ＴＳヘッダ、ＰＥＳヘッダ並びにシーケンスヘッダ、ＧＯＰヘッダ及びシーケンスエンドコードを暗号化せず、トランスポートストリームの他の部分のみを暗号化する。

【0037】

図５に、本発明の実施形態によるパーソナルコンピュータをベースとしたＭＰＥＧ信号

の処理システムを示す。

【0038】

図５を参照すると、このシステムは、ＣＰＵ１０１、ハードディスクドライブ１０２、デジタル放送処理ボード１０３、汎用バス１０４、表示部１０５及び編集部１０６を備える。

【0039】

ＣＰＵ１０１は、プログラムに従って、各種演算処理を行う。ハードディスクドライブ１０２は、各種プログラムやデータを格納し、特に、暗号化されたトランスポートストリームを格納する。デジタル放送処理ボード１０３は、デジタル放送されてきたトランスポートストリームの各種処理を行う。汎用バス１０４は、ＣＰＵ１０１、ハードディスクドライブ１０２、デジタル放送処理ボード１０３及び編集部１０６に接続され、これらの間で入出力するデータを運ぶ。表示部１０５は、各種画面を表示し、特にデジタル放送処理ボード１０３から入力した映像信号に従って映像を表示する。

【0040】

デジタル放送処理ボード１０３は、受信部１１１、暗号化部１１２、暗号解読部１１３、ＭＰＥＧデコーダ１１４、検出部１１５及び代表画像生成部１１６を備える。

【0041】

受信部１１１は、放送よりトランスポートストリームを受信する。検出部１１５は、受信部１１１が受信したトランスポートストリームからＴＳヘッダ、ＰＥＳヘッダ、シーケンスヘッダ並びにＧＯＰヘッダ及びシーケンスエンドコードを検出する。暗号化部１１２は、受信部１１１が受信したトランスポートストリームのうちＴＳヘッダ、ＰＥＳヘッダ並びにシーケンスヘッダ、ＧＯＰヘッダ及びシーケンスエンドコードを除く部分を暗号化して、一部が暗号化されたトランスポートストリームを汎用バス１０４に出力する。ハードディスクドライブ１０２は、この一部が暗号化されたトランスポートストリームを格納する。ハードディスクドライブ１０２は、格納されている一部が暗号化されたトランスポートストリームを出力し、暗号解読部１１３は、この一部が暗号化されたトランスポートストリームの暗号解読を行い、暗号解読されたトランスポートストリームから映像部分を多重分離したＭＰＥＧビットストリームをＭＰＥＧデコーダ１１４に出力する。ＭＰＥＧデコーダ１１４は、ＭＰＥＧビットストリームを復号して、これにより得た映像信号を表示部１０５に出力する。

【0042】

編集部１０６は、検出部１０６－１を備える。検出部１１５は、暗号化されていないトランスポートストリームからＴＳヘッダ、ＰＥＳヘッダ並びにシーケンスヘッダ、ＧＯＰヘッダ及びシーケンスエンドコードを検出するのに対し、検出部１０６－１は、ハードディスクドライブ１０２に格納されている一部が暗号化されているトランスポートストリームからＴＳヘッダ、ＰＥＳヘッダ並びにシーケンスヘッダ、ＧＯＰヘッダ及びシーケンスエンドコードを検出する。一部が暗号化されているトランスポートストリームのＴＳヘッダ、ＰＥＳヘッダ並びにシーケンスヘッダ、ＧＯＰヘッダ及びシーケンスエンドコードは暗号化されていないので、検出部１０６－１は、検出部１１５と同様な方法により、ハードディスクドライブ１０２に格納されている一部が暗号化されているトランスポートストリームからＴＳヘッダ、ＰＥＳヘッダ並びにシーケンスヘッダ、ＧＯＰヘッダ及びシーケンスエンドコードを検出することができる。そして、編集部１０６は、検出部１０６－１が検出したＧＯＰに含まれているタイムコードを基準にして、一部が暗号化されているトランスポートストリームのうち必要なＴＳパケットのみを、暗号解読せずに寄せ集めて、新たな一部が暗号化されたトランスポートストリームを生成し、生成された一部が暗号化されたトランスポートストリームをハードディスクドライブ１０２に書き込む。従って、ハードディスクドライブ１０２と編集部１０６と間では、一部が暗号化されたトランスポートストリームがやり取りされることより、汎用バス１０４には暗号解読されたトランスポートストリームは現れず、コンテンツの著作権を保護することができる。

【0043】

編集部１０６は、タイムコードを基準として編集を行うが、これのみでは、ユーザインターフェースが取れない。そこで、代表画像生成部１１６を設けている。受信部１１１がトランスポートストリームを受信している時に、ＭＰＥＧデコーダ１１４は、映像信号及びタイムコードを復元する。代表画像生成部１１６は、ＭＰＥＧデコーダ１１４から復元映像信号及びタイムコードを入力し、全部又は一部（例えば、シーンチェンジ部）のＧＯＰについて、復元映像信号から代表画像（例えば、ＧＯＰの最初のフレームのサムネイル）を作成し、その代表画像とタイムコードを関連付けて、ハードディスクドライブ１０２に書き込む。編集時には、編集部１０６は、代表画像を所定の方法により表示し、代表画像を用いて選択された範囲のタイムコードのＧＯＰを寄せ集める。

【0044】

また、一旦、一部が暗号化されたトランスポートストリームがハードディスクドライブ１０２に格納された後に、ハードディスクドライブ１０２から一部が暗号化されたトランスポートストリームを読み出し、暗号解読部１１３で暗号解読し、ＭＰＥＧデコーダ１１４で映像信号及びタイムコードを復元し、代表画像生成部１１６で代表画像を生成し、ハードディスクドライブ１０２に代表画像とタイムコードを関連付けて書き込んでもよい。

【0045】

また、暗号化部１１２が暗号化を行う際、ＧＯＰ毎に暗号鍵を変化させてもよい。

【0046】

具体的には、ＧＯＰのうちＩピクチャを暗号化し、Ｉピクチャ以外のピクチャを暗号化しない。そして、Ｉピクチャ以外のピクチャにＩピクチャの暗号解読をするために必要な暗号鍵を電子透かしの形態で埋め込んでおく。暗号解読の際には、まず、Ｉピクチャ以外のピクチャから電子透かしを検出し、検出された電子透かしから暗号鍵を抽出し、その暗号鍵を用いてＩピクチャを暗号解読する。Ｉピクチャの暗号解読ができない限り、Ｉピクチャ以外のピクチャを復元することができないので、Ｉピクチャを暗号化するのみで、ＧＯＰ全体を暗号化したのと同様な効果を得ることができる。

【0047】

又は、ＧＯＰのタイムコードとそのＧＯＰを暗号解読するために必要な暗号鍵を対応付けたテーブルをデジタル放送処理ボード１０３の不揮発性メモリ（図示せず）に書き込んでおいて、再生時に、そのテーブルを用いてＧＯＰ毎に暗号解読を行うようにしてもよい。

【0048】

又は、ＧＯＰのタイムコードとデジタル放送処理ボード１０３の不揮発メモリに書き込んである一定個数の暗号鍵のテーブルとの対応が取れる計算式に従い、そのＧＯＰの暗号鍵としてもよい。さらに、デジタル放送処理ボード１０３の基本となる暗号鍵とＧＯＰのタイムコードを元に計算式によってＧＯＰ毎の暗号鍵を生成してもよい。

【0049】

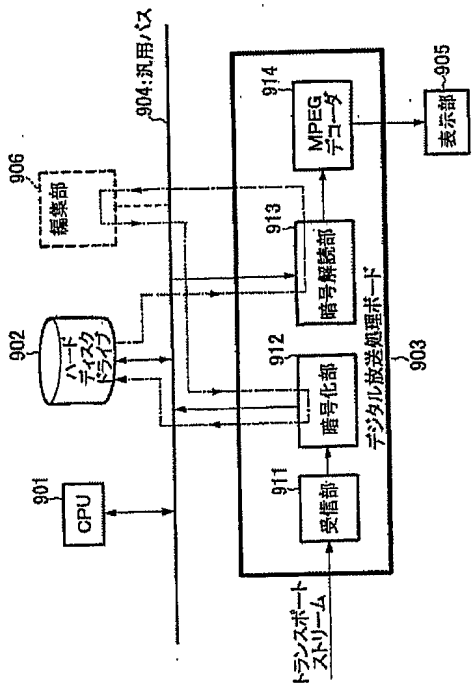
なお、受信部１１１、暗号化部１１２、暗号解読部１１３、ＭＰＥＧデコーダ１１４、検出部１１５及び代表画像生成部１１６は、ハードウェアによって実現してもよいし、デジタル放送処理ボード１０３に搭載したＣＰＵが、このＣＰＵをこれらの部分として機能させるためのプログラムを実行することによって実現してもよい。また、編集部１０６及び検出部１０６－１は、ハードウェアによって実現してもよいし、ＣＰＵ１０１が、このＣＰＵをこれらの部分として機能させるためのプログラムを実行することによって実現してもよい。

【0050】

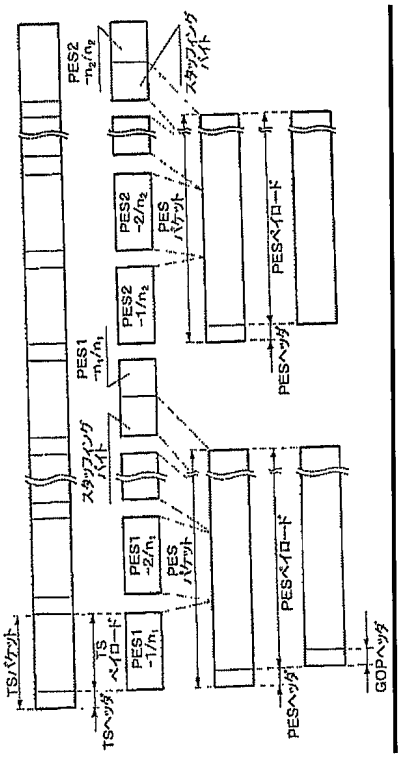
上記の説明では、トランスポートストリームを扱うこととしたが、上記と同様な考えの基にプログラムストリームを処理しても良い。すなわち、パックヘッダ、ＰＥＳヘッダ、シーケンススタートコード、ＧＯＰヘッダ及びシーケンスエンドコードを除いてプログラムストリームを暗号化し、そのようなプログラムストリームからパックヘッダ、ＰＥＳヘッダ、シーケンススタートコード、ＧＯＰヘッダ及びシーケンスエンドコードを検出し、暗号解読しないでＧＯＰ単位でプログラムポートストリームの編集を行う。

【産業上の利用可能性】
【0051】
本発明は、コンテンツの著作権を保護した状態で、コンテンツを編集することに利用することができる。
【図面の簡単な説明】
【0052】
【図1】従来例によるパーソナルコンピュータをベースとしたＭＰＥＧ信号の処理システムの構成を示すブロック図である。
【図2】ＴＳパケットのフォーマット図である。
【図3】ＧＯＰとＰＥＳパケットとの関係を示す図である。
【図4】シーケンス層とＧＯＰ層との関係を示す図である。
【図5】本発明の実施形態によるパーソナルコンピュータをベースとしたＭＰＥＧ信号の処理システムの構成を示すブロック図である。
【符号の説明】
【0053】
１０１　ＣＰＵ
１０２　ハードディスクドライブ
１０３　デジタル放送処理ボード
１０４　汎用バス
１０５　表示部
１０６　編集部
１０６－１　検出部
１１１　受信部
１１２　暗号化部
１１３　暗号解読部
１１４　ＭＰＥＧデコーダ
１１５　検出部
１１６　代表画像生成部

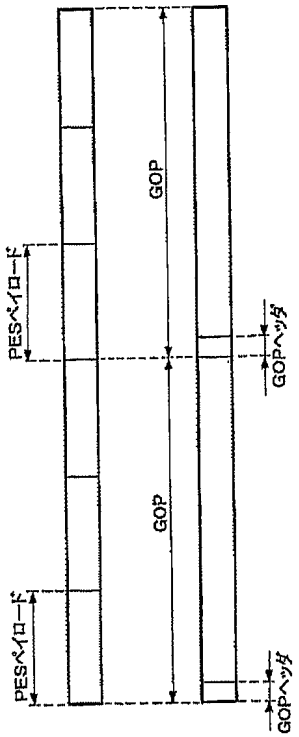
【図1】


904:汎用バス
906
編集部
902
ハードディスクドライブ
901
CPU
914
MPEGデコーダ
913
暗号解読部
912
暗号化部
911
受信部
903
デジタル放送処理ボード
905
表示部
トランスポートストリーム

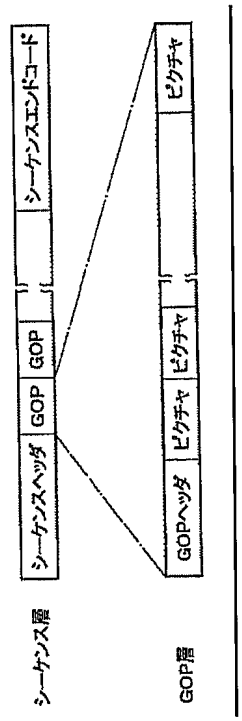
【図2】


PES2
スタッフィングバイト
PES2 -2/n2
PESパケット
PES2 -1/n2
PESヘッダ
PESペイロード
PES1 -n1/n1
PES1 -2/n1
PES1 -1/n1
TSパケット
TSヘッダ
TSペイロード
GOPヘッダ

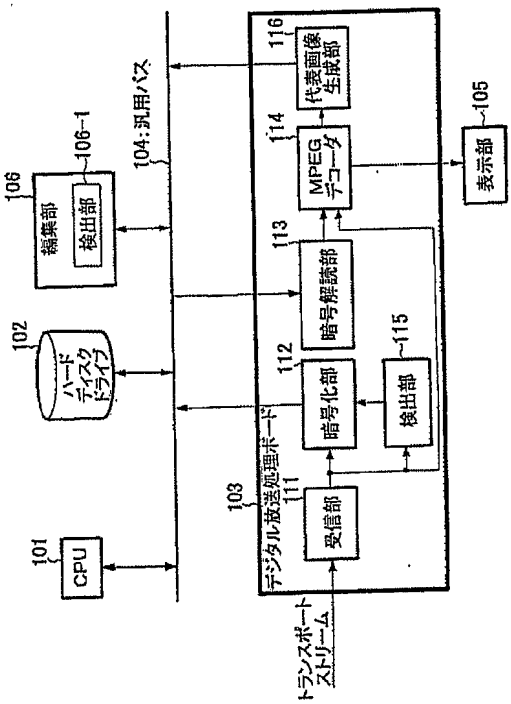
【図3】


PESペイロード
GOP
GOPヘッダ
PESペイロード
GOP
GOPヘッダ

【図4】


シーケンスエンドコード
シーケンスヘッダ
GOP
GOP
ピクチャ
ピクチャ
GOPヘッダ
ピクチャ
シーケンス層
GOP層

【図5】


101
CPU
102
ハードディスクドライブ
103
デジタル放送処理ボード
104:汎用バス
105
表示部
106
録画部
106-1
検出部
111
受信部
112
暗号化部
113
暗号解読部
114
MPEGデコーダ
115
検出部
116
代表画像生成部
トランスポートストリーム

Ｆターム(参考) 5C053 FA14 FA23 GA11 GB05 GB21 GB37 KA01 KA24 LA06 LA15
5C064 CA14
5J104 AA12

【要約の続き】